IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	Michael Freed; Elango Ganesan; Praveen Patnala	Confirmation No.	4141
Serial No.:	09/900,515		
Filed:	July 6, 2001	Customer No.:	28863
Examiner:	Aravind K. Moorthy		
Group Art Unit:	2131		
Docket No.:	1014-056US01/JNP-0251		
Title:	SECURE SOCKETS LAYER CUT THROUGH ARCHITECTURE		

REPLY BRIEF

Board of Patent Appeals and Interferences
Commissioner for Patents
Alexandria, VA 22313-1450

Sir:

    This is a Reply Brief from the Examiner's Answer mailed May 29, 2008. It is believed that no fee is due for this matter. Please charge Deposit Account No. 50-1778 for any additional charges.

TABLE OF CONTENTS

REAL PARTY OF INTEREST

The Real Party of Interest is Juniper Networks, Inc., of Sunnyvale, California.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences for the above-referenced patent application.

STATUS OF CLAIMS

The Examiner accepted Appellant's statement in the Appeal Brief filed February 7, 2007.

STATUS OF AMENDMENTS

The Examiner accepted Appellant's statement in the Appeal Brief filed February 7, 2007.

SUMMARY OF CLAIMED SUBJECT MATTER

The Examiner accepted Appellant's statement in the Appeal Brief filed February 7, 2007.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

As stated in the Appellant's Appeal Brief, Appellant submits the following grounds of rejection to be reviewed on Appeal:

1. The first ground of rejection to be reviewed on appeal is the rejection of claims 1-8, 11, 45-47, 51 and 53 as anticipated under 35 U.S.C. § 102(e) by U.S. Patent No. 6,484,257 to Ellis.

2. The second ground of rejection to be reviewed on appeal is the rejection of claims 20-22, 27, 29, 33-35, 38, 39, 41 and 52 under 35 U.S.C. 103(a) as being unpatentable over Ellis in view of Maloney et al. (USPN 6,253,337).

ARGUMENT

In response to the Examiner's Answer, Appellant requests consideration of the following arguments, which supplement the arguments presented in the Appeal Brief. In the "Grounds of Rejection" section of the Examiner's Answer, the Examiner appears to have advanced the same arguments and rejections presented in the final Office Action. Appellant directs the Board of Patent Appeals to Appellant's original Appeal Brief, which addresses the rejections.

The following discussion is responsive to the "Response to Argument" section starting at pg. 27 of the Examiner's Answer.

The First Ground of Rejection to be Reviewed on Appeal

Claims 1-8, 11, 45-47, 51 and 53 stand rejected under 35 U.S.C. 102(e) as being anticipated by Ellis (USPN 6,484,257). Appellant separately argues independent claims 1 and 45 and dependent claims 3, 51 and 53.

Independent claim 1

In Appellant's Appeal Brief, Appellant first noted that claim 1 recites a method that requires managing a communications negotiation between the client and the server through an intermediate device that supports both a direct mode and a proxy mode. Appellant further noted that claim 1 also requires forwarding unencrypted data packets from the intermediate device to the server using a communication session <u>negotiated by the client and the server</u> when the intermediate device operates in <u>direct</u> mode.

In the Examiner's Answer, pg. 27, the Examiner argued that Ellis teaches "*forwarding unencrypted data packets from the intermediate device to the server using a communication session negotiated by the client and the server when the intermediate device operates in direct mode.*" Specifically, on pg. 27, the Examiner argued that Ellis teaches these elements of claim 1 as follows:

> "*Ellis discloses that the client authenticates to the main serer. Ellis discloses that the (Main) server gets the client information including the bandwidth requirements to*

4

determine how many agents to assign to the client [column 8, lines 29-32]. Ellis
discloses that the Agent server (i.e., the intermediate device) decrypts session
communication and redirects this decrypted communications to the intended final
destination (i.e., the client or Main Server) [column 7, lines 57-59]. ... As discussed, Ellis
discloses a communication session negotiated by the client and server."

The Examiner's conclusions are inconsistent with the description of Ellis. Specifically, to the
extent the Agent server can be viewed as an intermediate device, as argued by the Examiner, the
Ellis system still does not teach forwarding unencrypted data packets from the intermediate
device to the server using a communication session negotiated by the client and the server when
the intermediate device operates in direct mode. According to the Examiner's reasoning, this
would require the Agent server (as the intermediate device) to have the ability to forward
unencrypted packets to the server (the "final destination" in Ellis) using a communication session
negotiated by the client and that final destination when the intermediate device operates in direct
mode. The Agent server in Ellis has no such feature.

First, on pg. 27, the Examiner states that the "intended final destination" to which the
Agent Sever forwards traffic in Ellis is "i.e., the client or the Main Server" and cites col. 7, ll. 57-
59. This is factually incorrect. Ellis does not refer to the Client or the Main Server as the final
destination. Rather, Ellis makes clear that the "final destinations" to which the Agent Server
forwards decrypted communications are other servers or devices within the network and not the
Client nor the Main Server. For example, at col. 6, ll. 10-13, Ellis first states that "the invention
uses client server and agent technology to establish end to end or 'final mile' security links to the
final destination inside the business network." Ellis at col. 7, ll. 57-59, the portion of Ellis cited
by the Examiner, then explains that:

> "*The Client will then begin encrypting its session communication to the Agent*
> *Server (via the Main Server gateway) using the key and information obtained from the*
> *Main Server. The Agent Server will decrypt the session communication and redirect this*
> *decrypted communication to the <u>intended final destination.</u>*"

Thus, Ellis makes clear that the Agent Server is intermediate between the Client and the intended
final destination of the Client, and that the Agent Server decrypts session communications from

the client and redirects those communications to that intended final destination. Thus, the Examiner is incorrect on pg. 27 in stating that the "intended final destination" to which the Agent Sever forwards traffic is "the Client or the Main Server" and citing col. 7, ll. 57-59.

Second, Ellis makes clear that the Client establishes a secure communication session with either the Main Server or an Agent Server:

> "First the Main Server starts up, wherein a registry is created and initialized and the server begins execution 402. The Agent Server(s) register themselves 405 with the Main Server and define session key(s) with which to establish secure communications. The Main Server and Agent Servers become enabled to receive secure connections from Clients 410 and 415. The Client(s) connects to the Main Server and authenticates using one of several servers known authentication methods 420. The Main Server determines if it can accept a new session based on its current available processor bandwidth. **If the Main Server can accept a new session based on available processor resources, _then it agrees on a secret session key with the Client(s) and begins the session(s)_. If the Main Server has insufficient resources to service the session 425, then it will instruct an Agent Server(s) to become unblocked [wake up] and participate in a multiparty key exchange between a Client, Main Server and Agent Server. ... _The Client and Agent will independently generate a session key to exchange data._**[1]

Thus, Ellis makes clear that the client does not negotiate a communication with the final destination, as argued by the Examiner. As such, the Agent Server operating as an intermediate device does not forward unencrypted data packets to the server (the final destination in Ellis) using a communication session negotiated by the client and the server (final destination) as argued by the Examiner. Thus, Ellis's use of an Agent Server does not anticipate forwarding unencrypted data packets from the intermediate device to the server using a communication session negotiated by the client and the server when the intermediate device operates in direct mode, as required by claim 1.

Further, with respect to the forwarding of packets by the Agent Server, Ellis goes on to describe the particular packet processing of the Agent Server as follows:

---

[1] Ellis, col. 7, ll. 17-54 (emphasis added).

6

The packet processing is shown in FIG. 5B. Again, the agent processed packets
are broken down into boxes to show the individual network model layer in each packet.
Note that the AGENT IP HEADER, ESP, AH and AGENT ID IP HEADER layers have
been stripped off by the agent. The remaining DATA 5B10, TCP 5B20, are pre-appended
a DESTINATION IP HEADER 5B30, and then forwarded to the final destination host
5B40, in FIG. 5B for reconstitution of individual packets.[2]

As explained by Ellis, the Agent Server adds a new destination header (DESTINATION IP
HEADER 5B30) to each of the packets so as to correctly direct the packets to the final
destination. The further serves to illustrate the conclusion that the Agent Server is not using a
communication session negotiated by the client and the final destination as argued by the
Examiner. If so, the Agent Server would not have to pre-append a new destination IP header to
the decrypted packets originating from the client, as those packets would already contain such
information. In summary, in the Examiner's Answer, pg. 27, the Examiner argues that Ellis
anticipates the claim elements of forwarding unencrypted data packets from the intermediate
device (Agent Server) to the server (final destination) using a communication session negotiated
by the client and the server (final destination) when the intermediate device (Agent Server)
operates in direct mode. This is factually unsupported by Ellis. Quite the contrary, Ellis makes
clear that the client negotiates with either the Main Server or the Agent Server and not the final
destination. Moreover, the packet processing described by Ellis further indicates that the Agent
Server does not forward unencrypted data packets to the server (final destination) using a
communication session negotiated by the client and the server (final destination) when the
intermediate device (Agent Server) operates in direct mode.

Further, as discussed in detail in Appellant Appeal Brief, claim 1 requires forwarding
unencrypted data packets from the intermediate device to the server using a communication
session negotiated by the server and the intermediate device when the intermediate device
operates in proxy mode. In response to Appellant's Argument, the Examiner on pg. 29, ll. 2-3,
stated only that "Ellis discloses that the main server authenticates an agent." This further
illustrates the Examiner's error. To the extent the Agent server is an intermediate device
between the Client and the final destination to which if forwards traffic (as argued by the

---

[2] Ellis, col. 9, ll. 24-30.

Examiner), the Agent server does not support a proxy mode as claimed by the Appellant. Claim 1 requires forwarding unencrypted data packets from the intermediate device to the server using a communication session negotiated by the server and the intermediate device when the intermediate device operates in proxy mode. In Ellis, the Agent Server forwards decrypted data to the "intended final destinations." The fact that the Agent Server may be authenticated by the Main Server is irrelevant as to how the Agent Server forwards decrypted data to the final destinations and as to what communication session that Agent Server uses. Thus, the Examiner's statement that "Ellis discloses that the main server authenticates an agent" provides no basis for concluding that Ellis anticipates forwarding unencrypted data packets from the intermediate device to the server using a communication session negotiated by the server and the intermediate device when the intermediate device operates in proxy mode. In Ellis, the Agent Server forwards decrypted data to the final destinations, and there is no description of that forwarding making use of a communication session negotiated by the server and the intermediate device when the intermediate device operates in proxy mode, as required by claim 1.

Claim 45

Finally, on pg. 28 in the Examiner's Answer with respect to claim 45, the Examiner summarily reads out elements of Applicant's claims. For example, the Examiner states that:

> *"The only difference in the two modes is that in direct mode negotiation takes place between the client and server and in proxy mode the negotiation takes place between the server and the intermediate devices."*

This overlooks the claim language that requires the claimed acceleration device to have a communication engine that is able to use two different types of communication sessions for forwarding decrypted data packets. Claim 45 literally requires that the communication engine supports: (1) a direct mode in which decrypted data packets are forwarded to the servers *using a communication session negotiated by the client and the server*, and (2) a proxy mode in which the acceleration device responds to the client on behalf of the server and forwards the decrypted data packets to the server *using the open communications session established by the acceleration device and the server*. The Examiner's arguments on pg. 28 of the Examiner's Answer overlook

8

these elements and effectively read these elements out of Appellant's claim 45. Neither the Agent Server nor any of the other components of the Ellis system have such features.

Dependent claim 3

The Examiner's arguments on pg. 29 of the Examiner's Answer fail to respond to the argument raised in Appellant's Appeal Brief. In the Appeal Brief, the Applicant pointed out that Ellis provides no support for the Examiner's conclusion that Ellis' decryption architecture teaches modification of SYN requests by decrypting them. Appellant noted that SYN requests are part of a TCP/IP handshake used to establish TCP/IP sessions. Consequently, only after a TCP/IP connection is established does a key exchange occur and can an SSL session be established. Encryption / decryption of data cannot occur until after the TCP/IP and SSL sessions are established, i.e., after the TCP handshake. There is no evidence in Ellis that the initial SYN requests in Ellis that establish TCP connections in the first place are in anyway "modified" from an encrypted form to a decrypted form, as suggested by the Examiner.

Dependent claims 51 and 53

With respect to claims 51 and 53, the Examiner on pg. 29 argued that Ellis' Main Server's ability to wake up Agent Servers anticipates automatically switching the intermediate device from the direct mode to the proxy mode upon detecting a communication error associated with the direct mode.

First, as discussed above, the Examiner erred in suggesting that Ellis' use of an Agent Server in the Ellis system supports a direct mode as required by the language of claims 1 or 45.

Second, as the Examiner first argued that use of the Agent Server constitutes a direct mode, it is inconsistent to now argue that invoking an Agent Server constitutes a switch *from* a direct mode to a *proxy mode*, as required by claim 51. This logic is seemingly backward.

Third, claim 51 requires automatically switching the intermediate device from the direct mode to the proxy mode *upon detecting a communication error associated with the direct mode*. This Examiner has pointed to no evidence of detecting a communication error with the direct mode. Quite the contrary, the Examiner argued that use of Agent Servers without interference of the Main Server is some form of a direct mode with respect to claim 1, and now argues that

9

switching to use of those Agent Servers anticipates automatically switching the intermediate device from the direct mode to the proxy mode *upon detecting a communication error associated with the direct mode*. Appellant points out that, even using the Examiner's interpretation of Ellis, the Main Server's determination of whether it has sufficient resources is not detection of a communication error nor is it a detection of a communication error associated with the direct mode, as required by claim 51.

Similarly, this provides no evidence for concluding that Ellis anticipates an acceleration device having a communications engine that automatically switches from the direct mode to the proxy mode upon detection of a communication error with the communication session negotiated by the client and the server. In response to the Examiner Answer at pg. 29, Appellant respectfully points out that Ellis' description of the Main Server's determining whether it has sufficient resources to accept a session provides no teaching or suggestion of automatically switching from the direct mode to a proxy mode, upon detection of a communication error with the communication session negotiated by the client and the server.

The Second Ground of Rejection to Be Reviewed on Appeal

Independent claims 20 and 33

Appellant argues claims 20 and 33 separately in Appellant Appeal Brief. The Examiner's response is deficient with respect to these claims for many of the reasons set forth above and those reasons set forth in Appellant's original Appeal Brief.
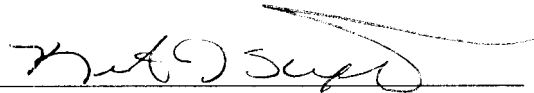
It is earnestly requested that the Examiner's rejection be reversed, and that all of the pending claims be allowed.

Date: By:

July 29, 2008
SHUMAKER & SIEFFERT, P.A.   Name: Kent J. Sieffert
1625 Radio Drive, Suite 300   Reg. No.: 41,312
Woodbury, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102

APPENDIX - CLAIMS ON APPEAL

The listing of the Claims on Appeal appears in Appellant's Appeal Brief filed February 7, 2007.

APPENDIX: EVIDENCE

None

APPENDIX: RELATED PROCEEDINGS

None